



*Office of the Director of National Intelligence*

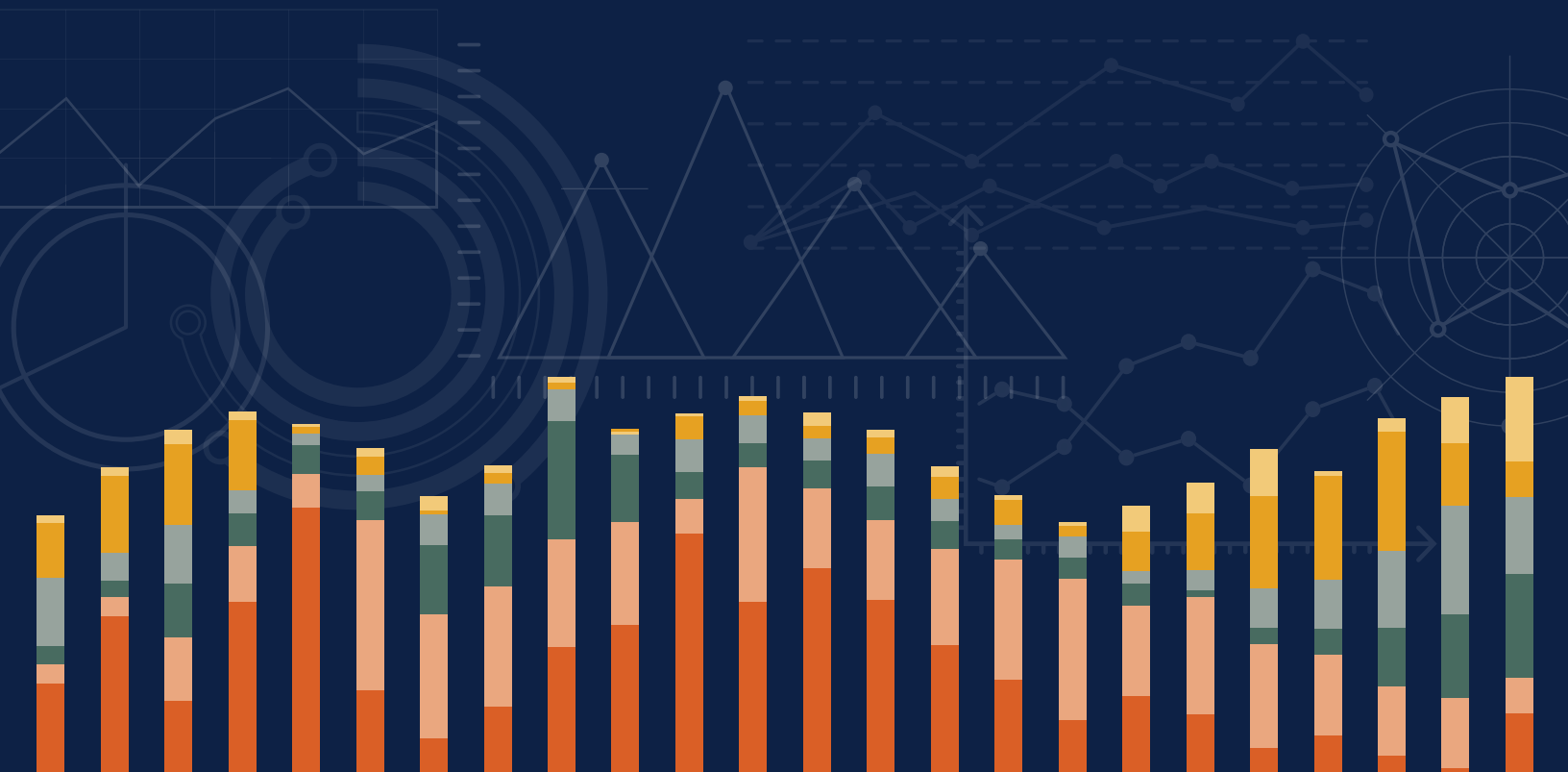
# STATISTICAL TRANSPARENCY REPORT

REGARDING THE USE OF NATIONAL SECURITY AUTHORITIES

Calendar Year 2018

Office of Civil Liberties, Privacy, and Transparency

April 2019



# Table of Contents

<b>Introduction .....</b>	<b>4</b>
<i>A. Background .....</i>	<i>4</i>
<i>B. Areas Covered in this Report .....</i>	<i>4</i>
<i>C. Context and Clarity.....</i>	<i>5</i>
<i>D. Key Terms .....</i>	<i>6</i>
<b>FISA Probable Cause Authorities .....</b>	<b>8</b>
<i>A. FISA Titles I and III.....</i>	<i>8</i>
<i>B. FISA Title VII, Sections 703 and 704.....</i>	<i>8</i>
<i>C. Statistics .....</i>	<i>8</i>
<b>FISA Section 702.....</b>	<b>10</b>
<i>A. Section 702 .....</i>	<i>10</i>
<i>B. Statistics—Orders and Targets.....</i>	<i>12</i>
<i>C. Statistics—U.S. Person Queries .....</i>	<i>13</i>
<i>D. Section 702 and FBI Investigations.....</i>	<i>16</i>
<i>E. NSA Dissemination of U.S. Person Information under FISA Section 702.....</i>	<i>17</i>
<b>FISA Criminal Use and Notice Provisions .....</b>	<b>22</b>
<i>A. FISA Sections 106 and 305 .....</i>	<i>22</i>
<b>FISA Title IV—Use of Pen Register and Trap and Trace (PR/TT) Devices.....</b>	<b>23</b>
<i>A. FISA PR/TT Authority.....</i>	<i>23</i>
<i>B. Statistics .....</i>	<i>23</i>
<b>FISA Title V—Business Records .....</b>	<b>25</b>
<i>A. Business Records FISA.....</i>	<i>25</i>
<i>B. Statistics—Title V “Traditional” Business Records Statistics Orders, Targets &amp; Identifiers .....</i>	<i>26</i>
<i>C. Statistics—Call Detail Record (CDR) Orders, Targets &amp; Identifiers.....</i>	<i>27</i>
<i>D. Statistics—Call Detail Record Queries .....</i>	<i>31</i>
<b>National Security Letters (NSLs).....</b>	<b>32</b>
<i>A. National Security Letters .....</i>	<i>32</i>
<i>B. Statistics—National Security Letters and Requests for Information.....</i>	<i>32</i>

# Table of Figures

<i>Figures 1a and 1b: FISA “Probable Cause” Court Orders and Targets .....</i>	<i>9</i>
<i>Figures 2a and 2b: FISA “Probable Cause” Targets Broken Down by U.S. Person Status .....</i>	<i>9</i>
<i>Figure 3: Section 702 Orders .....</i>	<i>13</i>
<i>Figure 4: Section 702 Targets .....</i>	<i>13</i>
<i>Figure 5: How the IC Counts U.S. Person Query Terms Used To Query Section 702 Content .....</i>	<i>14</i>
<i>Figure 6: U.S. Person Query Terms Used To Query Section 702 Content .....</i>	<i>14</i>
<i>Figure 7: How the IC Counts U.S. Person Query Terms Used To Query Section 702 Noncontents .....</i>	<i>15</i>
<i>Figure 8: U.S. Person Queries of Noncontents of Section 702 .....</i>	<i>15</i>
<i>Figure 9: Required Section 702 Query Reporting to the FISC.....</i>	<i>16</i>
<i>Figure 10: Number of FBI Investigations Opened on USPs Based on Section 702 Acquisition .....</i>	<i>16</i>
<i>Figure 11: Section 702 Reports Containing USP Information Unmasked by NSA.....</i>	<i>20</i>
<i>Figure 12: Section 702 USP Identities Disseminated by NSA .....</i>	<i>20</i>
<i>Figure 13: Number of Criminal Proceedings in Which the Government Provided Notice of Its Intent To Use Certain FISA Information .....</i>	<i>22</i>
<i>Figures 14a and 14b: Number of PR/TT Orders, Targets and Unique Identifiers Collected.....</i>	<i>24</i>
<i>Figure 15: FISA PR/TT Targets—U.S. Persons and Non-U.S. Persons.....</i>	<i>24</i>
<i>Figure 16a: Title V “Traditional” Business Records Orders, Targets, and Unique Identifiers Collected.....</i>	<i>26</i>
<i>Figure 16b: “Traditional” Business Records Orders and Targets .....</i>	<i>27</i>
<i>Figure 16c: “Traditional” Business Records Unique Identifiers.....</i>	<i>27</i>
<i>Figures 17a and 17b: CDR Orders and Targets .....</i>	<i>28</i>
<i>Figure 18: Call Event Hop Scenario and Method of Counting .....</i>	<i>29</i>
<i>Figure 19: CDRs Received Arising from Such Targets .....</i>	<i>30</i>
<i>Figure 20: Unique Identifiers in the CDRs Received .....</i>	<i>31</i>
<i>Figure 21: CDRs—U.S. Person Query Terms .....</i>	<i>31</i>
<i>Figure 22a: NSLs Issued and Requests for Information .....</i>	<i>33</i>
<i>Figure 22b: Total NSLs Issued and Total ROIs Within Those NSLs .....</i>	<i>33</i>

# Introduction

Today, consistent with the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended (codified in 50 U.S.C. § 1873(b)), and the Intelligence Community's (IC) [Principles of Intelligence Transparency](#), we are releasing our sixth annual *Statistical Transparency Report Regarding Use of National Security Authorities* presenting statistics on how often the government uses certain national security authorities. Providing these statistics allows for an additional way to track the use of FISA authorities and National Security Letters (NSLs). The statistics also add further context regarding the IC's rigorous and multi-layered oversight framework that safeguards the privacy of United States person (U.S. person or USP) information and non-U.S. persons' information acquired pursuant to these national security authorities. This report goes beyond the government's statutory duty of providing statistics by further providing the public with detailed explanations as to how the IC uses its national security authorities. This document should be read in conjunction with the national security-related materials that the government has already released publicly, especially the documents that have been highlighted through the hyperlinks embedded in this report, as well as the statistical report provided by the Director of the Administrative Office of the U.S. Courts (50 U.S.C. § 1873(a), available on the [AOUSC website](#)).

Additional public information on national security authorities is available at the Office of the Director of National Intelligence's (ODNI) website, [www.dni.gov](#), the Intelligence Community's public website, [www.intel.gov](#), and ODNI's public Tumblr site, [IC on the Record](#) at [IContheRecord.tumblr.com](#).

## A. Background

In June 2014, the Director of National Intelligence (DNI) began releasing statistics relating to the use

of critical national security authorities, including FISA, in an annual report called the *Statistical Transparency Report Regarding Use of National Security Authorities* (hereafter the *Annual Statistical Transparency Report*). Subsequent *Annual Statistical Transparency Reports* were released in [2015](#), [2016](#), [2017](#), and [2018](#).

On June 2, 2015, the Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act) was enacted, amending FISA by requiring the government to publicly report many of the statistics already reported in the *Annual Statistical Transparency Report*. The USA FREEDOM Act also expanded the scope of the information included in the reports by requiring the DNI to report information concerning USP search terms and queries of certain FISA-acquired information, as well as specific statistics concerning call detail records. See 50 U.S.C. § 1873(b). On January 19, 2018, the FISA Amendments Reauthorization Act of 2017 was signed, further codifying that additional statistics must be publicly released, including many statistics that the government previously reported pursuant to its commitment to transparency.

## B. Areas Covered in this Report

This report provides statistics in the following areas (the terms used below are defined and explained later in this report):

- **FISA PROBABLE CAUSE AUTHORITIES.** The number of orders—and the number of targets under those orders—for the use of FISA authorities that require probable cause determinations by the Foreign Intelligence Surveillance Court (FISC), under Titles I and III, and Section 703 and 704, of FISA.

## ■ FISA SECTION 702.

- ▶ The number of orders—and the number of targets under those orders—issued pursuant to Section 702 of FISA.
- ▶ The number of U.S. person queries of Section 702-acquired content.
- ▶ The number of U.S. person queries of Section 702-acquired metadata.
- ▶ The number of instances in which Federal Bureau of Investigation (FBI) personnel received and reviewed Section 702-acquired information that the FBI identified as concerning a U.S. person in response to a query that was designed to return evidence of a crime unrelated to foreign intelligence and conducted in connection with a predicated criminal investigation.
- ▶ The number of instances in which the FBI opened, under the Criminal Investigative Division, an investigation of a U.S. person who is not considered a threat to national security based wholly or in part on Section 702-acquired information.
- ▶ The number of National Security Agency (NSA)-disseminated Section 702 reports containing U.S. person identities (various statistics relating to reports where the U.S. person identity was openly named or originally masked and subsequently unmasked).

- **USE IN CRIMINAL PROCEEDINGS.** The number of criminal proceedings in which the United States or a State or political subdivision provided notice under FISA of the government's intent to enter into evidence or otherwise use or disclose any information derived from electronic surveillance, physical search, or Section 702 acquisition.

- **PEN REGISTER AND TRAP AND TRACE DEVICES.** The number of orders—and the number of targets under those orders—for the use of FISA's pen register/trap and trace devices, and the number

of unique identifiers used to communicate information collected pursuant to those orders.

- **BUSINESS RECORDS.** The number of business records are reported with distinction made between records obtained under Section 501(b)(2)(B)—commonly referred to as “traditional” business records—and call detail records obtained under Section 501(b)(2)(C). Specifically:

- ▶ The number of traditional business record orders—and the number of targets under those orders—issued pursuant to FISA's traditional business records authority, and the number of unique identifiers used to communicate information collected pursuant to those orders.
- ▶ The number of call detail record orders—and the number of targets under those orders—issued pursuant to FISA's call detail records authority for the ongoing production of call detail records, the number of call detail records received from providers and stored in NSA repositories, and the number of unique identifiers used to communicate information collected.

- **NATIONAL SECURITY LETTERS.** The number of National Security Letters (NSLs) issued, and the number of requests for information within those NSLs.

## C. Context and Clarity

Consistent with the IC's [Principles of Intelligence Transparency](#), and in addition to the mandatory reporting required by FISA, this report provides transparency to enhance public understanding about certain activities the IC undertakes to accomplish its national security mission. Specifically, this report provides context concerning how the IC implements FISA, including the circumstances under which such activities are conducted and the rules that are designed to ensure compliance with the Constitution and laws of the United States. While the statistics contained herein provide an important point for understanding the use of these authori-



ties, the statistics have limitations in explaining the complexities of how the IC implements FISA; thus, this report is intended to be read in conjunction with other related publicly released information for a more comprehensive understanding. The statistics fluctuate from year to year for a variety of reasons. These include changes in operational priorities, world events, technical capabilities, target behavior, the dynamics of the ever-changing telecommunications sector, and the use of technology to automate the delivery of marketing and other communications. These reasons often cannot be explored in detail in an unclassified setting without divulging information necessary to protect national security. Moreover, there may be no relationship between a decrease in the use of one authority and an increase in another.

## D. Key Terms

Certain terms used throughout this report are described below. Other terms are described in the sections in which they are most directly relevant. These terms will be used consistently throughout this report.

- **U.S. PERSON.** As defined by Title I of FISA, a U.S. person is “a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in [50 U.S.C. § 1801(a)(1), (2), or (3)].” 50 U.S.C. § 1801(i). Section 602 of the USA FREEDOM Act, however, uses a narrower definition. Since the broader Title I definition governs how U.S. person queries are conducted pursuant to the relevant minimization procedures, it will be used throughout this report.

- **TARGET.** Within the IC, the term “target” has multiple meanings. With respect to the statistics provided in this report, the term “target” is used as a noun and defined as the individual person, group, entity composed of multiple individuals, or foreign power that uses the selector such as a telephone number or email address.

The IC also uses the term “target” as a verb, especially as it relates to Section 702. Specifically, Section 702 authorizes the targeting of (i) non-United States persons (ii) reasonably believed to be located outside the United States (iii) to acquire foreign intelligence information. To ensure that all three requirements are appropriately met, Section 702 requires targeting procedures. Additional information on targeting is detailed below in the Section 702 discussion.

Targeting for intelligence purposes must be informed by the [National Intelligence Priorities Framework \(NIPF\)](#). The NIPF is the high-level mechanism to manage and communicate national intelligence priorities, facilitating the IC’s ability to allocate finite resources to address the most pressing intelligence questions and mission requirements. Guidance from the President and the National Security Advisor, with formal input from cabinet-level heads of departments and agencies, determine the overall priorities of the top-level NIPF issues. Once the IC determines that a particular target meets an intelligence need under the NIPF, the IC must then apply applicable legal authorities (e.g., certain acquisitions authorized under FISA, Executive Order 12333) to begin targeting.

- **ORDERS.** There are different types of orders that the FISC may issue in connection with FISA cases, including orders granting or modifying the government’s applications to conduct foreign intelligence collection including orders granting or modifying the government’s applications to conduct foreign intelligence collection pursuant to FISA; orders directing electronic

communication service providers to provide any technical assistance necessary to implement the authorized foreign intelligence collection; and supplemental orders and briefing orders requiring the government to take a particular action or provide the court with specific information. As with past years, this report only counts orders granting the government's applications.

The FISC may *amend* an order one or more times after it has been granted. For example, an order may be amended to add a newly discovered account used by the target. *This report does not count such amendments separately.*

The FISC may *renew* some orders multiple times during the calendar year. Each authority permitted under FISA has specific time limits for the FISA authority to continue (e.g., a Section 704 order against a U.S. person target outside of the United States may last no longer than 90 days, but FISA permits the order to be renewed, *see* 50 U.S.C. § 1881c(c)(4)). Each renewal requires a separate application submitted by the government to the FISC and a finding by the FISC that the application meets the requirements of FISA. Thus, unlike amendments, *this report counts each such renewal as a separate order granting the requested FISA authority.*

- **"ESTIMATED NUMBER."** Throughout this report, when numbers are *estimated*, the estimate comports with the statutory requirements to provide a "good faith estimate" of a particular number.
- **DISSEMINATION.** Dissemination refers to the sharing of minimized information. As it pertains to FISA (including Section 702), if an agency (such as NSA) lawfully collects information pursuant to

FISA and wants to disseminate that information, the agency must first apply its minimization procedures to that information.

- **FISC.** The FISC was established in 1978 when Congress enacted FISA (*see* 50 U.S.C. §§ 1801-1885c). The Court is composed of eleven federal district court judges who are designated by the Chief Justice of the United States. Pursuant to FISA, the Court entertains applications submitted by the United States Government for approval of electronic surveillance, physical search, and other investigative actions for foreign intelligence purposes.
- **AMICUS CURIAE.** In 2015, the USA FREEDOM Act established a framework under which qualified individuals are appointed as amicus curiae to assist the FISC and the Foreign Intelligence Surveillance Court of Review (FISC-R) in the consideration of matters (including matters that present a novel or significant interpretation of the law or matters dealing with technical expertise) before those courts. *See* 50 U.S.C. § 1803. Individuals designated as amici must have expertise in privacy and civil liberties, intelligence collection, communications technology, or other areas that may lend legal or technical expertise to the FISC and FISC-R and must also be eligible for access to classified information. When appointed, amicus curiae provide those courts, as appropriate, with legal arguments that advance the protection of individual privacy and civil liberties; information related to intelligence collection or communications technology; or legal arguments or information regarding any other area relevant to the issue presented to the court.

# FISA Probable Cause Authorities

## A. FISA Titles I and III

**With limited exceptions (e.g., in the event of an emergency), to conduct electronic surveillance or physical search of an individual under FISA Title I or FISA Title III, a probable cause court order is required regardless of U.S. person status.**

Under FISA, Title I permits electronic surveillance and Title III permits physical search in the United States of foreign powers or agents of a foreign power when the government has a significant purpose to obtain foreign intelligence information. See 50 U.S.C. §§ 1804 and 1823. Title I (electronic surveillance) and Title III (physical search) are commonly referred to as “Traditional FISA.” Both require that, following submission of a government application, the FISC make a probable cause finding, based upon a factual statement in the government’s application, that (i) the target is a foreign power or an agent of a foreign power, as defined by FISA and (ii) the facility being targeted for electronic surveillance is used by or about to be used, or the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power. In addition to meeting the probable cause standard, the government’s application must meet the other requirements of FISA. See 50 U.S.C. §§ 1804(a) and 1823(a).

## B. FISA Title VII, Sections 703 and 704

**FISA Title VII Sections 703 and 704 similarly require a court order based on a finding of probable cause for the government to undertake FISA collection targeting U.S. persons located outside the United States.**

Section 703 applies when the government seeks to conduct electronic surveillance or to acquire stored electronic communications or stored electronic data inside the U.S., in a manner that otherwise requires an order pursuant to FISA, of a U.S. person who is reasonably believed to be located outside the United States. Section 704 applies when the government

### FISA Title I, Title III, and Title VII Section 703 and 704

- All of these authorities require individual court orders based on probable cause.
- Titles I and III apply to FISA collection targeting persons within the United States.
- Sections 703 and 704 apply to FISA collection targeting U.S. persons outside the United States.

seeks to conduct collection overseas targeting a U.S. person reasonably believed to be located outside the United States under circumstances in which the U.S. person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted in the United States. Both Sections 703 and 704 require that the FISC make a probable cause finding, based upon a factual statement in the government’s application, that the target is a U.S. person reasonably believed to be (i) located outside the United States and (ii) a foreign power, agent of a foreign power, or officer or employee of a foreign power. Additionally, the government’s application must meet the other requirements of FISA. See 50 U.S.C. §§ 1881b(b) and 1881c(b).

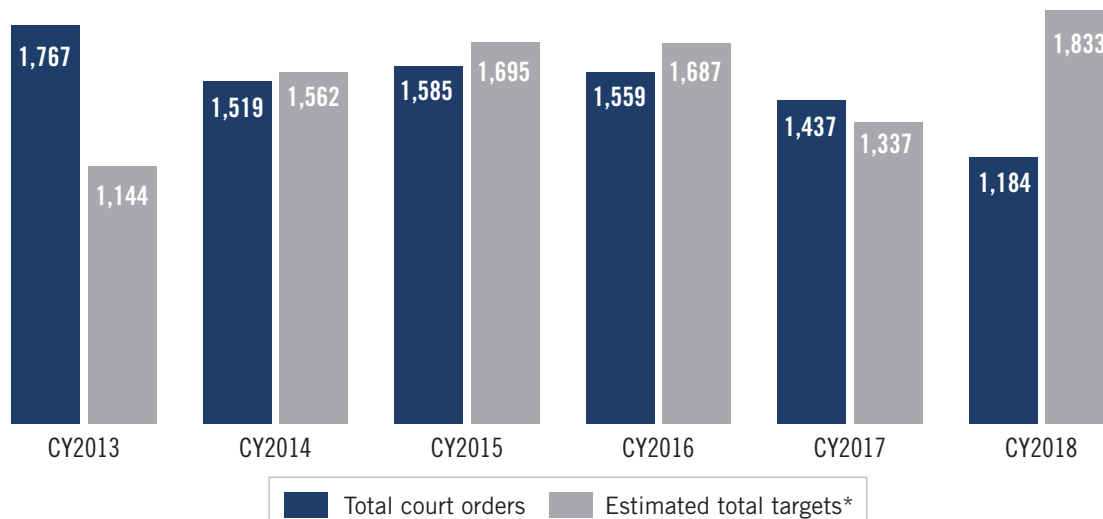
## C. Statistics

**HOW TARGETS ARE COUNTED.** If the IC received authorization to conduct electronic surveillance and/or physical search against the same target in four separate applications, the IC would count one target, not four. Alternatively, if the IC received authorization to conduct electronic surveillance and/or physical search against four targets in the same application, the IC would count four targets. Duplicate targets across authorities are not counted.



**Figures 1a and 1b: FISA “Probable Cause” Court Orders and Targets**

Titles I and III and Sections 703 and 704 of FISA	CY2013	CY2014	CY2015	CY2016	CY2017	CY2018
Total number of orders	1,767	1,519	1,585	1,559	1,437	<b>1,184</b>
Estimated number of targets of such orders*	1,144	1,562	1,695	1,687	1,337	<b>1,833</b>



See 50 U.S.C. §§ 1873(b)(1) and 1873(b)(1)(A).

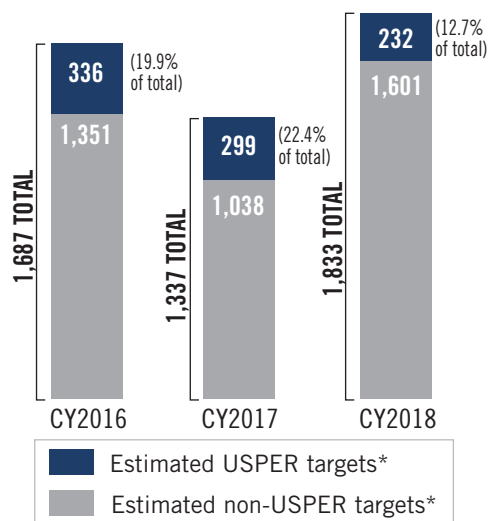
\*Although providing this statistic was first required by the USA FREEDOM Act, the FISA Amendments Reauthorization Act of 2017 enumerated this requirement at 50 U.S.C. § 1873(b)(1)(A).

**Figures 2a and 2b: FISA “Probable Cause” Targets Broken Down by U.S. Person Status**

Titles I and III and Sections 703 and 704—Targets	CY2016	CY2017	CY2018
Estimated number of targets who are <i>non</i> -U.S. persons*	1,351	1,038	<b>1,601</b>
Estimated number of targets who are U.S. persons*	336	299	<b>232</b>
Percentage of targets who are estimated to be U.S. persons	19.9%	22.4%	<b>12.7%</b>

See 50 U.S.C. §§ 1873(b)(1)(B) and 1873(b)(1)(C) for rows one and two, respectively.

\*Previously the IC was not statutorily required to publicly provide these statistics but provided them consistent with transparency principles. The FISA Amendments Reauthorization Act of 2017 codified this requirement at 50 U.S.C. §§ 1873(b)(1)(B) and 1873(b)(1)(C).



# FISA Section 702

## A. Section 702

**T**itle VII of FISA includes Section 702, which permits the Attorney General and the DNI to jointly authorize the targeting of (i) non-U.S. persons (ii) who are reasonably believed to be located outside the United States (iii) to acquire foreign intelligence information. *See* 50 U.S.C. § 1881a. *All three* elements must be met. Additionally, Section 702 requires that the Attorney General, in consultation with the DNI, adopt targeting procedures, minimization procedures, and querying procedures that they attest satisfy the statutory requirements of Section 702 and are consistent with the Fourth Amendment. Additional information on how the government uses Section 702 is posted on [IC on the Record](#) including a [Section 702 Overview](#).

**SECTION 702 TARGETS AND “TASKING.”** Under Section 702, the government “targets” a particular non-U.S. person, including non-U.S. person groups or entities, reasonably believed to be located outside the United States to acquire foreign intelligence information by “tasking” selectors (e.g., telephone numbers and email addresses). Before tasking a selector for collection under Section 702, the government must apply its targeting procedures to ensure that the selector is used by a non-U.S. person who is reasonably believed to be located outside the United States and who is expected to possess, receive, and/or is likely to communicate foreign intelligence information. The foreign intelligence information must fall within a specific category of foreign intelligence information that has been authorized for acquisition by the Attorney General and the DNI as part of a Section 702 certification.

In addition to the requirement that the type of foreign intelligence information sought must be authorized as part of a certification approved by the FISC, agencies must also apply protections

### FISA Title VII— Section 702

- Commonly referred to as “Section 702.”
- Requires individual targeting determinations that the target (1) is a non-U.S. person (2) who is reasonably believed to be located outside the United States and (3) who has or is expected to communicate or receive foreign intelligence information.

required by [Presidential Policy Directive 28 \(PPD-28\)](#), Signals Intelligence Activities, to Section 702-acquired information. PPD-28 reinforces longstanding intelligence practices that protect privacy and civil liberties, while requiring agencies to implement new procedures to ensure that U.S. signals intelligence activities continue to include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides.

NSA and FBI task selectors pursuant to their respective Section 702 targeting procedures, which are discussed below. All agencies that receive unminimized (i.e., “raw”) Section 702 data—NSA, FBI, Central Intelligence Agency (CIA), and National Counterterrorism Center (NCTC)—handle the Section 702-acquired data in accordance with minimization procedures, which are explained below.

**THE FISC’S ROLE.** Under Section 702, the FISC determines whether certifications executed jointly by the Attorney General and the DNI meet all the requirements of Section 702. In deciding whether to approve a certification application package, the FISC reviews the certifications and the minimization, targeting, and querying procedures to ensure compliance with both FISA and the Fourth Amendment.

The Court's review is not limited to the procedures as written, but also includes an examination of how the procedures have been and will be implemented. Accordingly, as part of its review, the FISC considers the compliance incidents reported to it by the government through notices and reports.

If the FISC determines that the government's certification application package meets the statutory requirements of Section 702 and are consistent with the Fourth Amendment, then the FISC issues an order and supporting statement approving the certifications. The [2016 FISC order and statement approving the certifications](#) was publicly released, in redacted form, in May 2017 and posted on *IC on the Record*.

**CERTIFICATIONS.** Under Section 702, the Attorney General and DNI jointly execute certifications under which the Intelligence Community intends to acquire specified foreign intelligence information. The certifications identify categories of foreign intelligence information to be collected, which must meet the statutory definition of foreign intelligence information, through the targeting of non-U.S. persons reasonably believed to be located outside the United States. The certifications have included information concerning international terrorism and other topics, such as the acquisition of information concerning weapons of mass destruction. Each annual certification must be submitted to the FISC for approval in a certification application package that includes the Attorney General and DNI's certifications, affidavits by certain heads of intelligence agencies, targeting procedures, minimization procedures, and, as described below, querying procedures. [Samples of certification application packages](#) have been publicly released on *IC on the Record*, most recently in [May 2017](#).

**TARGETING PROCEDURES.** Each set of targeting procedures are adopted by the Attorney General and then reviewed, as part of the certification package, by the FISC, which reviews the sufficiency of each agency's targeting procedures including assessing the IC's compliance with the procedures. Only

agencies that have Attorney General-adopted targeting procedures that the FISC finds sufficient as part of a certification package may task selectors pursuant to Section 702; only two agencies, NSA and FBI, have targeting procedures and thus are permitted to task selectors.

NSA includes the targeting rationale (TAR) in the tasking record, which requires the targeting analyst to briefly state why targeting for a particular selector was requested. The intent of the TAR is to memorialize why the analyst is requesting targeting and provide a linkage between the user of the selector and the foreign intelligence purpose covered by the certification under which it is being tasked. The TAR is reviewed by the ODNI and Department of Justice oversight teams as part of their routine review of the tasking records. More information about these oversight reviews is provided in the Attorney General and DNI's joint [Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act](#) (commonly referred to as the *Joint Assessment of 702 Compliance* or *Joint Assessment*), most recently released in February 2019 on *IC on the Record*. [NSA's 2016 targeting procedures](#) and [FBI's 2016 targeting procedures](#) have been publicly released on *IC on the Record*.

**MINIMIZATION PROCEDURES.** The minimization procedures detail requirements the government must meet to use, retain, and disseminate Section 702 data, including specific restrictions regarding non-publicly available U.S. person information acquired from Section 702 collection of non-U.S. person targets, consistent with the needs of each agency to obtain, produce, and disseminate foreign intelligence information. Each agency's Section 702 minimization procedures are adopted by the Attorney General. The FISC reviews the sufficiency of each agency's minimization procedures as part of the certification application package. Such reviews include assessing the IC's compliance with past procedures. The [2016 minimization procedures](#) have been released on *IC on the Record*.

Non-U.S. persons also benefit from many of the protective rules prescribed by the targeting and minimization procedures. Under Section 702, collection is targeted (not bulk), and must be limited to non-U.S. person targets located outside the United States who are likely to possess, receive, and/or are expected to communicate foreign intelligence information that is linked to one of the FISC-approved certifications. See [Status of Implementation of PPD-28: Response to the PCLOB's Report, October 2018](#) at 9. Additionally, “as a practical matter, non-U.S. persons also benefit from the access and retention restrictions required by the different agencies’ minimization and/or targeting procedures.” See [Privacy and Civil Liberties Oversight Board Report on the Surveillance Program Operated Pursuant to Section 702 of FISA](#) (July 2, 2014) at 100.

**QUERYING PROCEDURES.** With passage of the FISA Amendments Reauthorization Act of 2017, Congress amended Section 702 to require that querying procedures be adopted by the Attorney General, in consultation with the DNI. Section 702(f)(1) requires that the querying procedures be consistent with the Fourth Amendment and that they include a technical procedure whereby a record is kept of each U.S. person term used for a query. Similar to the Section 702 targeting and minimization procedures, the querying procedures are required to be reviewed by the FISC as part of the certification package for consistency with the statute and the Fourth Amendment. Congress added other requirements in Section 702(f), which pertain to accessing certain results of queries conducted by FBI; those requirements will be discussed later in this report.

Query terms may be date-bound, and may include alphanumeric strings, such as telephone numbers, email addresses, or terms, such as a name, that can be used individually or in combination with one another. Pursuant to court-approved procedures, an agency can only query Section 702 information if the query is reasonably likely to return foreign intelligence information or, in the case of the FBI, evidence of a crime. This standard applies to all

Section 702 queries, regardless of whether the term includes U.S. person or non-U.S. person identifiers. As explained in the March 2019-released [Joint Assessment of Section 702 Compliance](#), NSA personnel are required to obtain Office of General Counsel approval before any use of United States person identifiers as terms to query the content of Section 702 information. Additional information about U.S. person queries is posted on *IC on the Record*.

**COMPLIANCE.** The IC’s application of the targeting, minimization, and querying procedures is subject to [robust internal agency oversight and to rigorous external oversight by DOJ, ODNI, Congress, and the FISC](#). Every identified incident of non-compliance, regardless of the U.S. person status of individuals affected by the incident, is reported to the FISC (through notices or in reports) and to Congress in semiannual reports. Depending on the nature of the incident, the FISC may order remedial actions, which could include deleting improperly collected information, recalling improperly disseminated information, and re-training IC employees. DOJ and ODNI also jointly submit semiannual reports to Congress that assess the IC’s overall compliance efforts. [Past Joint Assessments of Section 702 Compliance](#) have been publicly released.

## B. Statistics—Orders and Targets

**COUNTING SECTION 702 ORDERS.** As explained above, the FISC may issue a single order to approve more than one Section 702 certification to acquire foreign intelligence information. Note that, in its own transparency report, which is required pursuant to 50 U.S.C. § 1873(a), the Director of the Administrative Office of the United States Courts (AOUSC) counted each of the Section 702 certifications associated with the FISC’s order. Because the number of the government’s Section 702 certifications remains a classified fact, the government requested that the AOUSC redact the number of certifications from its transparency report prior to publicly releasing it.



**Figure 3: Section 702 Orders**

Section 702 of FISA	CY2013	CY2014	CY2015	CY2016	CY2017	CY2018
Total number of orders issued	1	1	1	0*	1	1

See 50 U.S.C. § 1873(b)(2).

\* In 2016, the government submitted a certification application package to the FISC. Pursuant to 50 U.S.C. § 1881a(j)(2), the FISC extended its review of the 2016 certification package. The FISC may extend its review of the certifications “as necessary for good cause in a manner consistent with national security.” See 50 U.S.C. § 1881a(j)(2), subsequently codified under § 1881a(k)(2) with the FISA Amendments Reauthorization Act of 2017. Thus, because the FISC did not complete its review of the 2016 certifications during calendar year 2016, the FISC did not issue an order concerning those certifications in calendar year 2016. The 2015 order remained in effect during the extension period. On April 26, 2017, the [FISC issued an order authorizing the 2016 certifications](#).

**ESTIMATING SECTION 702 TARGETS.** The number of 702 targets, provided below, reflects an estimate of the number of non-U.S. persons who are the users of tasked selectors. This estimate is based on information readily available to the IC. Unless and until the IC has information that links multiple selectors to a single foreign intelligence target, each individual selector is counted as a separate target for purposes

of this report. On the other hand, where the IC is aware that multiple selectors are used by the same target, the IC counts the user of those selectors as a single target. This counting methodology reduces the risk that the IC might inadvertently understate the number of discrete persons targeted pursuant to Section 702.

**Figure 4: Section 702 Targets\***

Section 702 of FISA	CY2013	CY2014	CY2015	CY2016	CY2017	CY2018
Estimated number of targets of such orders**	89,138	92,707	94,368	106,469	129,080	164,770

See 50 U.S.C. § 1873(b)(2)(A).

\*Recall that only non-USPs are targeted

\*\*Previously the IC was not statutorily required to publicly provide this statistic but provided it consistent with transparency principles. The FISA Amendments Reauthorization Act of 2017 codified this requirement at 50 U.S.C. § 1873(b)(2)(A).

### C. Statistics—U.S. Person Queries

In July 2014, the Privacy and Civil Liberties Oversight Board (PCLOB or Board) issued a report on Section 702 entitled, “*Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*” (PCLOB’s *Section 702 Report*), which reported U.S. person query statistics for calendar year 2013. See PCLOB’s *Section 702 Report* at 57-58. The USA FREEDOM Act, enacted in 2015, added a requirement to report publicly certain statistics regarding the number of U.S. person que-

ries of Section 702. Specifically, the Act requires reporting of the “number of search terms concerning a known United States person used to retrieve the unminimized contents [...]”—referred to as “query terms of content”—and “the number of queries concerning a known United States person of unminimized noncontents information [...]”—referred to as “queries of metadata.” See 50 U.S.C. § 1873(b)(2)(B) and (b)(2)(C), respectively. Thus, ODNI began reporting on these statistics in the *Annual Statistical Transparency Report* covering [CY2015](#).

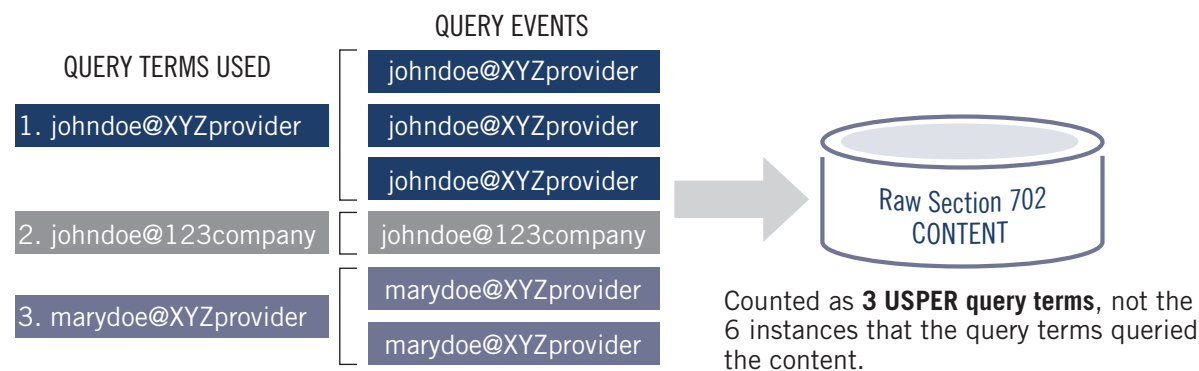


Below are statistics for U.S. person queries of raw, Section 702-acquired data.<sup>1</sup> The U.S. person statistics are based on (a) U.S. person *query terms* used to query Section 702 *content* and (b) U.S. person *queries* conducted of Section 702 *noncontents* (i.e., metadata). It is important to understand that these two very different numbers cannot be combined because they use *different counting methodologies* (query terms versus queries conducted) and *different data types* (content versus noncontents).

**COUNTING U.S. PERSON QUERY TERMS USED TO QUERY SECTION 702 CONTENT.** The NSA counts the number of U.S. person identifiers it approved to query the content

of unminimized Section 702-acquired information. For example, if the NSA used U.S. person identifier “johndoe@XYZprovider” to query the content of Section 702-acquired information, the NSA would count it as one regardless of how many times the NSA used “johndoe@XYZprovider” to query its 702-acquired information. The CIA started using this model in 2016 for counting query terms and those statistics were included in the *Annual Statistical Transparency Report* covering [CY2016](#). When the NCTC began receiving raw Section 702 information, NCTC followed a similar approach of counting U.S. person query terms that were used to query Section 702 content.

**Figure 5: How the IC Counts U.S. Person Query Terms Used To Query Section 702 Content**



**Figure 6: U.S. Person Query Terms Used To Query Section 702 Content**

Section 702 of FISA	CY2015	CY2016	CY2017	CY2018
Estimated number of search terms concerning a known U.S. person used to retrieve the unminimized contents of communications obtained under Section 702 (excluding search terms used to prevent the return of U.S. person information)*	4,672	5,288	7,512	<b>9,637</b>

See 50 U.S.C. § 1873(b)(2)(B).

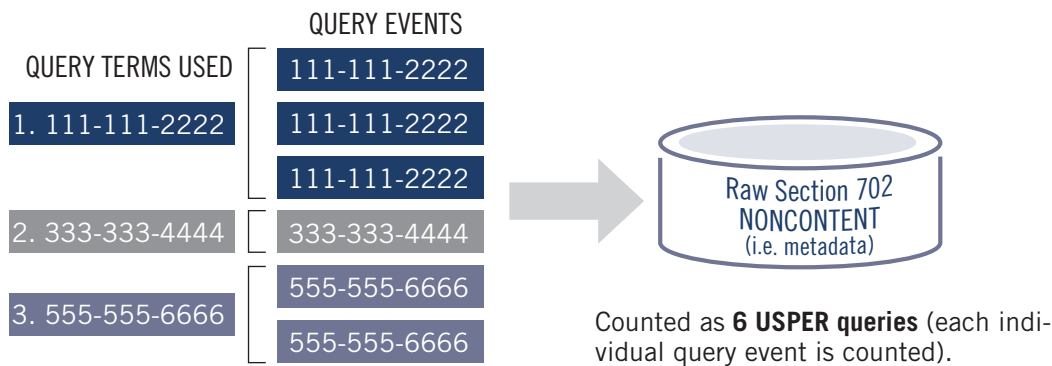
\*Consistent with 50 U.S.C. § 1873(d)(2)(A), this statistic does not include queries that are conducted by the FBI.

<sup>1</sup> With the FISA Amendments Reauthorization Act in 2017, Congress codified new requirements regarding the access to results of certain queries conducted by the FBI. Specifically under Section 702(f)(2)(A), an order from the FISC is now required before the FBI can review the contents of a query using a U.S. person query term when the query was not designed to find and extract foreign intelligence information and was performed in connection with a predicated criminal investigation that does not relate to national security. Before the FISC may issue such an order based on a finding of probable cause, an FBI agent must apply in writing, to include the agent's justification that the query results would provide evidence of criminal activity, and the application must be approved by the Attorney General. 50 U.S.C. Section 1873(b)(2)(A) requires annual reporting of the number of times the FBI received an order pursuant to 702(f)(2)(A).

**COUNTING QUERIES USING U.S. PERSON IDENTIFIERS OF NONCONTENTS COLLECTED UNDER SECTION 702.** This estimate represents the number of times a U.S. person identifier is used to query the noncontents (i.e., metadata) of unminimized Section 702-ac-

quired information. For example, if the U.S. person identifier telephone number “111-111-2222” was used 15 times to query the noncontents of Section 702-acquired information, the number of queries counted would be 15.

**Figure 7: How the IC Counts U.S. Person Query Terms Used To Query Section 702 Noncontents**



The CIA, had been previously unable to provide the number of queries using U.S. person identifiers of unminimized Section 702 noncontents information. Beginning in 2018, CIA was able to

estimate the number of these queries and, as such, this new information is included in the CY2018 statistic below.

**Figure 8: U.S. Person Queries of Noncontents of Section 702**

Section 702 of FISA	CY2013	CY2014	CY2015	CY2016	CY2017	CY2018**
Estimated number of queries concerning a known U.S. person of unminimized noncontent information obtained under Section 702 (excluding queries containing information used to prevent the return of U.S. person information)*	9,500	17,500	23,800	30,355	16,924	<b>14,374</b>

See 50 U.S.C. § 1873(b)(2)(C).

\*Consistent with 50 U.S.C. § 1873(d)(2)(A), this statistic does not include queries that are conducted by the FBI.

\*\*Beginning with CY2018, this statistic includes all elements that are required to report this number. As explained above, prior to CY2018, CIA had been unable to provide this number.

**FISC ORDER REQUIRING CERTAIN SECTION 702 QUERY REPORTING BY FBI.** On November 6, 2015, the FISC granted the government’s application for renewal of the 2015 certifications and, among other things, concluded that the FBI’s U.S. person querying provisions in its minimization procedures, “strike a reasonable balance between the privacy interests of the United States persons and persons in the United States, on the one hand, and the government’s national security interests, on the other.” *Memorandum Opinion and Order dated November 6, 2015*, at 44 (released on *IC on the Record* on April 19, 2016). The FISC further stated that the FBI conducting queries, “designed to return evidence of crimes unrelated to foreign intelligence does not preclude the Court from concluding that taken together, the targeting and minimization procedures submitted with the 2015 Certifications are consistent with the requirements of the Fourth Amendment.” *Id.*

Nevertheless, the FISC ordered the government to report in writing, “each instance after December 4, 2015, in which FBI personnel *receive and review* Section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information.” (Emphasis added). *Id.* at 44 and 78. The FISC directed that the report contain details of the query terms, the basis for conducting the query, the manner in which the query will be or has been used, and other details. *Id.* at 78. In keeping with the IC’s Principles of Intelligence Transparency, the DNI declassified the number of each such query reported to the FISC in calendar year 2016 and for applicable calendar years thereafter. These numbers are reported in Figure 9.

**Figure 9: Required Section 702 Query Reporting to the FISC**

Section 702 of FISA	CY2016	CY2017	CY2018
Per the FISC Memorandum Opinion and Order dated November 6, 2015: Each reported instance in which FBI personnel <i>received and reviewed</i> Section 702-acquired information that the FBI identified as concerning a U.S. person in response to a query that was designed to return evidence of a crime unrelated to foreign intelligence.	1	0	0

See FISC Memorandum Opinion and Order dated November 6, 2015.

### D. Section 702 and FBI Investigations

With the enactment of the FISA Amendments Reauthorization Act of 2017, FISA now requires that the FBI report on the number of instances in which the FBI opened, under the Criminal Investigative Division, a criminal investigation of a U.S. person, who is not considered a threat to national security, based wholly or in part on Section

702-acquired information. See 50 U.S.C. § 1873(b)(2)(D). This statistic will provide transparency with regard to how often Section 702 collection is used for non-national security investigations conducted by the FBI. Figure 10 provides the required statistic.

**Figure 10: Number of FBI Investigations Opened on USPs Based on Section 702 Acquisition**

Section 702 of FISA	CY2017	CY2018
The number of instances in which the FBI opened, under the Criminal Investigative Division or any successor division, an investigation of a U.S. person (who is not considered a threat to national security) based wholly or in part on an acquisition authorized under Section 702.	0	0

See 50 U.S.C. § 1873(b)(2)(D).

## E. NSA Dissemination of U.S. Person Information under FISA Section 702

**BACKGROUND ON NSA DISSEMINATING U.S. PERSON INFORMATION UNDER SECTION 702.** In July 2014, the PCLOB's *Section 702 Report* contained 10 recommendations. Recommendation 9 focused on "accountability and transparency," noting that the government should implement measures, "to provide insight about the extent to which the NSA acquires and utilizes the communications involving U.S. persons and people located in the United States under the Section 702 program." PCLOB's *Section 702 Report* at 145-146. Specifically, the PCLOB recommended that "the NSA should implement processes to annually count [...] (5) the number of instances in which the NSA disseminates non-public information about U.S. persons, specifically distinguishing disseminations that includes names, titles, or other identifiers, such as telephone numbers or e-mail addresses, potentially associated with individuals." *Id.* at 146. This recommendation is commonly referred to as Recommendation 9(5). In response to the PCLOB's July 2014 Recommendation 9(5), NSA previously publicly provided (in the *Annual Statistical Transparency Report* for calendar year 2015) and continues to provide the following additional information regarding the dissemination of Section 702 intelligence reports that contain U.S. person information. Because the PCLOB issued its recommendation in 2014, these statistics were not included in *Annual Statistical Transparency Report* for calendar years 2013 or 2014.

NSA has been providing similar information to Congress since 2009, in classified form, per FISA reporting requirements. For example, FISA Section 702(m)(3) requires that NSA annually submit a report to applicable Congressional committees regarding certain numbers pertaining to the acquisition of Section 702-acquired information, including the number of "disseminated intelligence reports containing a reference to a United States person identity." See 50 U.S.C. § 1881a(m)(3)(A)

(i) (prior to the FISA Amendments Reauthorization Act of 2017 under § 1881a(l)(3)(A)(i)). Section 702(m)(3)(A) also requires that the number of "United States-person identities subsequently disseminated by [NSA] in response to request for identities that were not referred to by name or title in the original reporting." See 50 U.S.C. § 1881a(m)(3)(A)(ii). This second requirement refers to NSA providing the number of approved unmasking requests, which is explained below. Additionally, the Attorney General and the DNI provide to Congress the number of NSA's disseminated intelligence reports containing a U.S. person reference as part of the Attorney General and the DNI's Joint Assessment of Compliance. See 50 U.S.C. § 1881a(m)(1) (prior to the FISA Amendments Reauthorization Act of 2017 under § 1881a(l)(1)).

Prior to the PCLOB issuing its *Section 702 Report*, NSA's Director of the Civil Liberties, Privacy, and Transparency Office published "NSA's Implementation of Foreign Intelligence Surveillance Act Section 702," on April 16, 2014, (hereinafter "[NSA DCLPO Report](#)"), in which it explained NSA's dissemination processes. *NSA DCLPO Report* at 7-8. NSA "only generates classified intelligence reports when the information meets a specific intelligence requirement, regardless of whether the proposed report contains U.S. person information." *NSA DCLPO Report* at 7.

Section 702 only permits the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information. Such targets, however, may communicate information to, from, or about U.S. persons. [NSA's minimization procedures](#) (publicly released on August 11, 2016) permit the NSA to disseminate U.S. person information if the information is necessary to understand the foreign intelligence. By policy, generally, the NSA masks the information that could identify the U.S. person. NSA's minimization procedures define U.S. person identi-



fying information as “(1) the name, unique title, or address of a United States person; or (2) other personal identifiers of a United States person [...]”. See NSA’s Minimization Procedures 2(f).

The minimization procedures also permit NSA to disseminate U.S. person identities only if doing so meets one of the specified reasons listed in NSA’s minimization procedures, including that the U.S. person consented to the dissemination, the U.S. person information was already publicly available, the U.S. person information was necessary to understand foreign intelligence information, or the communication contained evidence of a crime and is being disseminated to law enforcement authorities. For example, a Section 702 target may communicate information about a U.S. person that the target intends to victimize in some way; NSA may need to disseminate the identity of affected U.S. persons to appropriate authorities so that they can take appropriate protective, preventive, or investigative action.

Even if one these conditions applies, as a matter of policy, NSA may still mask the U.S. person identity and will include no more than the minimum amount of U.S. person information necessary to understand the foreign intelligence or to describe the crime or threat. *Id.* In certain instances, however, NSA makes a determination that it is appropriate to include in the original report the U.S. person’s identity, using the same standards discussed above.

- **MASKED U.S. PERSON INFORMATION.** Agency minimization procedures generally provide for the substitution of a U.S. person identity with a generic phrase or term if the identity otherwise does not meet the dissemination criteria; this is often referred to as “masking” the identity of the U.S. person. Information about a U.S. person is masked when the identifying information about the person is not included in a report. For example, instead of reporting that Section 702-acquired information revealed that non-U.S. person “Bad Guy” communicated with

U.S. person “John Doe” (i.e., the actual name of the U.S. person), the report would mask “John Doe’s” name, and would state that “Bad Guy” communicated with “an identified U.S. person,” “a named U.S. person,” or “a U.S. person.” Other examples of masked U.S. person identities would be “a named U.S. entity,” “a U.S. person email address,” or “a U.S. IP address.”

- **UNMASKING U.S. PERSON INFORMATION.** Recipients of NSA’s classified reports, such as other federal agencies, may request that NSA provide the U.S. person identifying information that was masked in an intelligence report. The requested identity information is released only if the requesting recipient has a “need to know” the identity of the U.S. person and if the dissemination of the U.S. person’s identity would be consistent with NSA’s minimization procedures (e.g., the identity is necessary to understand foreign intelligence information or assess its importance), and additional approval has been provided by a designated NSA official.

As part of their regular oversight reviews, DOJ and ODNI review disseminations of information about U.S. persons that NSA obtained pursuant to Section 702 to ensure that the disseminations were consistent with the minimization procedures.

Additional information describing how the IC protects U.S. person information obtained pursuant to FISA provisions is provided in [recent reports](#) by the civil liberties and privacy officers for the ODNI (including NCTC), NSA, FBI, and CIA. The reports collectively documented the rigorous and multi-layered framework that safeguards the privacy of U.S. person information in FISA disseminations. See [ODNI Report on Protecting U.S. Person Identities in Disseminations under FISA](#) and [annexes containing agency specific reports](#).

**STATISTICS OF NSA’S U.S. PERSON DISSEMINATING INFORMATION.** Below are statistics and charts to further explain how NSA disseminates U.S. person infor-



mation incidentally acquired from Section 702 in classified intelligence reports. NSA may:

- i. openly name (i.e., originally reveal) the U.S. person identity in the report,
- ii. initially mask (i.e., not reveal) the U.S. person identity in the report, or
- iii. in the instances where the U.S. person identity was initially masked, upon a specific request, later reveal and unmask the U.S. person identity but only to the requestor.

Consistent with the [CY2017 Annual Statistical Transparency Report](#), this year's report presents the dissemination numbers in a different format from the CY2016 and prior year reports to facilitate understanding and to provide consistency with NSA's classified FISA Section 702(m)(3) reports to Congress. This report separates the number of *reports* (in Figure 11) from the statistics relating to the U.S. person identities later disseminated (in Figure 12).

NSA applies its minimization procedures in preparing its classified intelligence reports, and then disseminates the reports to authorized recipients with a need to know the information in order to perform their official duties. Very few of NSA's intelligence reports from Section 702 collection contain references to U.S. person identities (whether masked or openly named).

The first row of Figure 11 provides "an accounting of the number of disseminated intelligence reports containing a reference to a United States-person identity." See 50 U.S.C. § 1881a(m)(3)(A)(i). NSA's counting methodology is to include any disseminated intelligence report that contains a reference to one or more U.S. person identities, whether masked or openly named, even if the report includes information from other sources. NSA does not maintain

records that allow it to readily determine, in the case of an intelligence report that includes information from several sources, from which source a reference to a U.S. person identity was derived. Accordingly, the references to U.S. person identities may have resulted from Section 702 authorized collection or from other authorized signals intelligence activity conducted by NSA. This counting methodology was used in the previous report and is used in NSA's FISA Section 702(m)(3) report.

Note that a single report could contain multiple U.S. person identities, masked and/or openly named. For example, a single report could include of a large number of U.S. identities that a foreign intelligence target is seeking to victimize; each of those identifiers would be counted.

As noted above, a U.S. person is "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in [50 U.S.C. § 1801(a)(1), (2), or (3)]." See 50 U.S.C. § 1801(i). Thus the numbers below include U.S. person identities not only of U.S. persons who are individuals, but also of U.S. persons that are corporations or unincorporated associations.

The second row of Figure 11 provides the *number of reports* containing U.S. person identities *where the U.S. person identity was masked* in the report. The third row provides the *number of reports* containing U.S. person identities *where the U.S. person identity was openly included* in the report.

**Figure 11: Section 702 Reports Containing USP Information Unmasked by NSA**

Section 702 Reports Containing U.S. Person (USP) Information Disseminated by NSA	CY2016	CY2017	CY2018
<b>REPORTS</b> —Total number of NSA disseminated § 702 reports containing USP identities <i>regardless of whether or not the identity was openly included or masked</i> .	3,914	4,065	<b>4,495</b>
<b>REPORTS</b> —Total number of NSA disseminated § 702 reports containing USP identities <i>where the USP identity was masked</i> .	2,964	3,034	<b>3,442</b>
<b>REPORTS</b> —Total number of NSA disseminated § 702 reports containing USP identities <i>where the USP identity was openly included</i> .	1,200	1,341	<b>1,379</b>

Rows 2 and 3 will not total row 1 because one report may contain both masked and openly named identities

Figure 12 provides statistics relating to the numbers of U.S. person *identities* that were originally masked in those reports counted in Figure 11 but which NSA later provided to authorized requestors (i.e., unmasked). This statistic is the number required to be reported to Congress in NSA's FISA Section 702(m)(3) report. In other words, Figure 12 provides "an accounting of the number of United States-person identities subsequently disseminated by [NSA] in response to requests for identities that were not referred to by name or title in the original reporting." See 50 U.S.C. § 1881a(m)(3)(A)(ii). This number is different than numbers provided in either CY2015 or the CY2016 *Annual Statistical Transparency Report*. NSA has decided to declassify the total number of U.S. person identities unmasked in response to a request.

The CY2015 and CY2016 *Annual Statistical Transparency Reports* focused on responding to

the PCLOB's report recommendation 9(5) by counting only those U.S. person identities where the proper name or title of an individual was unmasked; it did not count other identifiers such as email addresses, telephone numbers or U.S. IP addresses; nor did it count identifiers pertaining to U.S. corporations or associations. Rather than distinguishing between the different ways a U.S. person might be named in an intelligence report, NSA now provides the total number of U.S. person identities unmasked in response to a specific request from another agency. This is the same metric that NSA reports to Congress pursuant to FISA Section 702(m)(3) reporting requirements. Prior to CY2017, NSA's FISA Section 702(m)(3) reports covered the time period of September through August. For CY2017 and going forward, both reports now cover the same timeframe and follow the same reporting methodology.

**Figure 12: Section 702 USP Identities Disseminated by NSA**

Section 702—U.S. Person (USP) Identities Unmasked by NSA	12-month period Sep 2015–Aug 2016	CY2017	CY2018
The number of U.S. person identities that NSA unmasked in response to a specific request from another agency	9,217	9,529	<b>16,721</b>

[Intelligence Community Policy Guidance \(ICPG\)](#)

107.1, Requests for Identities of U.S. Persons in Disseminated Intelligence Reports, requires all IC elements to have procedures to respond to requests for the identities of U.S. persons whose identities were originally masked in a disseminated intelligence report. ICPG 107.1 applies to information regardless of the legal authority under which the information was collected (i.e., including, but not limited to, FISA Section 702). The ICPG further

requires the DNI to report, on an annual basis, certain statistics to track requests made pursuant to ICPG 107.1.

Since issuance of ICPG 107.1, all IC elements have finalized their procedures. As of January 1, 2019, all IC elements began tracking the applicable requests. Accordingly, ODNI will be able to provide these numbers for CY2019 in next year's *Annual Statistical Transparency Report*.

CONTENTS

FIGURES

INTRODUCTION

FISA PROBABLE CAUSE AUTHORITIES

FISA SECTION 702

FISA CRIMINAL USE

FISA TITLE IV

FISA TITLE V

NATIONAL SECURITY LETTERS

# FISA Criminal Use and Notice Provisions

## A. FISA Sections 106 and 305

FISA Section 106 requires *advance* authorization from the Attorney General *before* any information acquired through Title I electronic surveillance may be used in a criminal proceeding. This authorization from the Attorney General is defined to include authorization by the Acting Attorney General, Deputy Attorney General, or, upon designation by the Attorney General, the Assistant Attorney General for National Security. Section 106 also requires that if a government entity intends to introduce into evidence in any trial, hearing, or other proceeding, against an “aggrieved person,” information obtained or derived from electronic surveillance, it must notify the aggrieved person and the court. The aggrieved person is then entitled to seek suppression of the information. FISA Section 706 requires that any information acquired pursuant to Section 702 be treated as electronic surveillance under Section 106, including for purposes of the use, notice, and suppression requirements.

FISA Section 305 provides comparable requirements for use of information acquired through Title III physical search (i.e., advance authorization, notice, and opportunity to suppress) in a legal proceeding.

## B. Statistics

The FISA Amendments Reauthorization Act of 2017 codified a requirement that certain statistics concerning criminal proceedings must be provided to the public pertaining to Sections 106 and 305,

### FISA Sections 106 and 305— Criminal Use and Notice Provisions

- Commonly referred to as the “criminal use provision.”
- Section 106 applies to information acquired from Title I electronic surveillance and Section 702; Section 305 applies to information acquired from Title III physical search.
- Attorney General advance authorization is required before such information may be used in a criminal proceeding; if such information is used or intended to be used against an aggrieved person, that person must be given notice of the information and have a chance to suppress the information.
- The FISA Amendments Reauthorization Act of 2017 codified that statistics must be provided to the public as it pertained to Section 106, Section 305, as well as Section 702 acquired information.

including Section 702-acquired information. Specifically, Figure 13 provides that the government filed notice of intent to use FISA-acquired information, pursuant to Section 106 or 305, in seven (7) separate proceedings in 2017 and in fourteen (14) separate criminal proceedings in 2018.

**Figure 13: Number of Criminal Proceedings in Which the Government Provided Notice of Its Intent To Use Certain FISA Information**

	CY2017	CY2018
The number of criminal proceedings in which the United States or a State or political subdivision thereof provided notice pursuant to Section 106 (including with respect to Section 702-acquired information) or Section 305 of the government's intent to enter into evidence or otherwise use or disclose any information obtained or derived from electronic surveillance, physical search, or Section 702 acquisition.	7	14

See 50 U.S.C. § 1873(b)(4).

# FISA Title IV—Use of Pen Register and Trap and Trace (PR/TT) Devices

## A. FISA PR/TT Authority

Title IV of FISA authorizes the use of pen register and trap and trace (PR/TT) devices for foreign intelligence purposes. Title IV authorizes the government to use a PR/TT device to capture dialing, routing, addressing or signaling (DRAS) information. The government may submit an application to the FISC for an order approving the use of a PR/TT device (i.e., PR/TT order) for (i) “any investigation to obtain foreign intelligence information not concerning a United States person or” (ii) “to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.” 50 U.S.C. § 1842(a). If the FISC finds that the government’s application meets the requirements of FISA, the FISC must issue an order for the installation and use of a PR/TT device.

## B. Statistics

**COUNTING ORDERS.** Similar to how orders were counted for Titles I and III and Sections 703 and 704, this report only counts the orders granting authority to conduct intelligence collection—the order for the installation and use of a PR/TT device. Thus, renewal orders are counted as a separate order; modification orders and amendments are not counted.

**ESTIMATING THE NUMBER OF TARGETS.** The government’s methodology for counting PR/TT targets is similar to the methodology described above for counting targets of electronic surveillance and/or physical search. If the IC received authorization for the installation and use of a PR/TT device against the same target in four separate applications, the IC would count one target, not four. Alternatively, if

## FISA Title IV

- Commonly referred to as the “PR/TT” provision.
- Bulk collection is prohibited.
- Requires individual FISC order to use PR/TT device to capture dialing, routing, addressing, or signaling (DRAS) information.
- Government request to use a PR/TT device on U.S. person target must be based on an investigation to protect against terrorism or clandestine intelligence activities and that investigation must not be based solely on the basis of activities protected by the First Amendment to the Constitution.

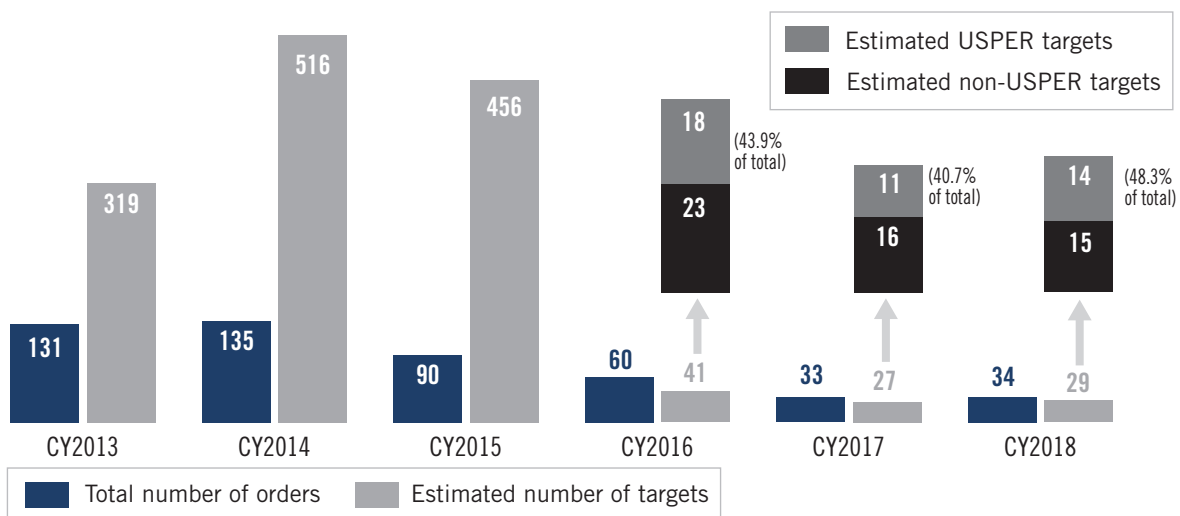
the IC received authorization for the installation and use of a PR/TT device against four targets in the same application, the IC would count four targets.

**ESTIMATING THE NUMBER OF UNIQUE IDENTIFIERS.** This statistic counts (1) the targeted identifiers and (2) the non-targeted identifiers (e.g., telephone numbers and email addresses) that were in contact with the targeted identifiers. Specifically, the House Report on the USA FREEDOM Act states that “[t]he phrase ‘unique identifiers used to communicate information collected pursuant to such orders’ means the total number of, for example, email addresses or phone numbers that have been collected as a result of these particular types of FISA orders—not just the number of target email addresses or phone numbers.” [H.R. Rept. 114-109 Part I, p. 26], with certain exceptions noted.



**Figures 14a and 14b: Number of PR/TT Orders, Targets and Unique Identifiers Collected**

Titles IV of FISA PR/TT FISA	CY2013	CY2014	CY2015	CY2016	CY2017	CY2018
Total number of orders	131	135	90	60	33	<b>34</b>
Estimated number of targets of such orders	319	516	456	41	27	<b>29</b>
Estimated number of unique identifiers used to communicate information collected pursuant to such orders*			134,987 <sup>•</sup>	81,035 <sup>•‡</sup>	56,064 <sup>•</sup>	<b>132,690</b>



See 50 U.S.C. §§ 1873(b)(3), 1873(b)(3)(A), and 1873(b)(3)(B).

\*Pursuant to § 1873(d)(2)(B), this statistic does not apply to orders resulting in the acquisition of information by the FBI that does not include email addresses or telephone numbers.

• This number represents information the government received from provider(s) electronically for the entire calendar year. The government does not have a process for capturing unique identifiers received by other means (such as hard-copy or portable media).

‡ For the CY2016 report, FBI erroneously provided the estimated number of unique identifiers used to communicate information collected pursuant to orders for *business records* instead of the number of the unique identifiers collected pursuant PR/TT orders. As noted below, FBI erroneously provided the estimated number of unique identifiers used to communicate information collected pursuant to orders for PR/TT orders under the statistics for business records.

**Figure 15: FISA PR/TT Targets—U.S. Persons and Non-U.S. Persons\***

PR/TT Targets	CY2016	CY2017	CY2018
Estimated number of targets who are <i>non-U.S.</i> persons*	23	16	<b>15</b>
Estimated number of targets who are U.S. persons	18	11	<b>14</b>
Estimated percentage of targets who are U.S. persons	43.9%	40.7%	<b>48.3%</b>

See 50 U.S.C. §§ 1873(b)(3)(A)(i) and 1873(b)(3)(A)(ii) for rows one and two, respectively.

\*Previously the IC was not statutorily required to publicly provide these statistics, but provided them consistent with transparency principles. The FISA Amendments Reauthorization Act of 2017 codified this requirement at 50 U.S.C. §§ 1873(b)(3)(A)(i) and 1873(b)(3)(A)(ii).

# FISA Title V—Business Records

## A. Business Records FISA

**T**itle V of FISA authorizes the government to submit an application for an order requiring the production of any tangible things for (i) “an investigation to obtain foreign intelligence information not concerning a United States person or” (ii) “to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.” 50 U.S.C. § 1861. Title V is commonly referred to as the “*Business Records*” provision of FISA.

In June 2015, the USA FREEDOM Act was signed into law and, among other things, it amended Title V, including by prohibiting bulk collection. *See* 50 U.S.C. §§ 1861(b), 1861(k)(4). The DNI is required to report various statistics about two Title V provisions—traditional business records under Section 501(b)(2)(B) and call detail records under Section 501(b)(2)(C). On November 28, 2015, in compliance with amendments enacted by the USA FREEDOM Act, the IC terminated collection of bulk telephony metadata under Title V of FISA (the “Section 215 Program”). Solely due to legal obligations to preserve records in certain pending civil litigation, the IC continues to preserve previously collected bulk telephony metadata. Under the terms of a FISC order dated November 24, 2015, the bulk telephony metadata cannot be used or accessed for any purpose other than compliance with preservation obligations. Once the government’s preservation obligations are lifted, the government is required to promptly destroy all bulk metadata produced by telecommunications providers under the Section 215 Program.

On November 30, 2015, the IC implemented certain provisions of the USA FREEDOM Act,

### FISA Title V

- Title V has two key provisions: (1) traditional business records and (2) Call Detail Records (CDRs).
- Request for records in an investigation of a U.S. person must be based on an investigation to protect against terrorism or clandestine intelligence activities and provided that the investigation is not conducted solely upon activities protected by the First Amendment to the Constitution.
- CDRs may be obtained from a telephone company if the FISC issues an individual court order for the target’s records.
- Bulk collection of CDRs is prohibited.

including the call detail records provision and the requirement to use a specific selection term. Accordingly, only one month’s worth of data for calendar year 2015 was available with respect to those provisions. Any statistical information relating to a particular FISA authority for a particular month remains classified. Therefore, the Title V data specifically associated with December 2015 was only released in a classified annex provided to Congress as part of the report for CY2015. After CY2015, statistical information was collected for an entire year and those statistics were included in subsequent reports.

Statistics related to traditional business records obtained under Title V Section 501(b)(2)(B) are provided first pursuant to 50 U.S.C. § 1873(b)(5). Statistics related to call detail records obtained under Title V Section 501(b)(2)(C) are provided second pursuant to 50 U.S.C. § 1873(b)(6).

## B. Statistics—Title V “Traditional” Business Records Statistics Orders, Targets & Identifiers

Business Record (BR) requests for tangible things may include books, records, (e.g. electronic communications transactions records), papers, documents, and other items pursuant to 50 U.S.C. § 1861(b)(2)(B), also referred to as Section 501(b)(2)(B). These are commonly referred to as traditional business records.

**ESTIMATING THE NUMBER OF UNIQUE IDENTIFIERS.** This is an estimate of the number of (1) targeted identifiers (e.g., telephone numbers and email addresses) and (2) non-targeted identifiers that were in contact with the targeted identifiers. The number of identifiers used by targets to communicate can vary significantly from year to year, which in turn will impact the number of non-targeted identifiers in contact with the targeted identifiers. Furthermore, this metric represents unique identifiers received electronically from the provider(s). The government does not have a process for capturing unique identifiers received by other means (i.e., hard-copy or portable media). For example, the FBI could obtain, under this authority, a hard-copy of a

purchase receipt from a company. That purchase receipt could contain a unique identifier such as a telephone number, which would not be counted.

**EXPLAINING HOW WE COUNT BR STATISTICS.** As an example of the government’s methodology, assume that in 2017, the government submitted a BR request targeting “John Doe” with email addresses john.doe@serviceproviderX, john.doe@service-providerY, and john.doe@serviceproviderZ. The FISC found that the application met the requirements of Title V and issued orders granting the application and directing service providers X, Y, and Z to produce business records pursuant to Section 501(b)(2)(B). Provider X returned 10 non-targeted email addresses that were in contact with the target; provider Y returned 10 non-targeted email addresses that were in contact with the target; and provider Z returned 10 non-targeted email addresses that were in contact with the target. Based on this scenario, we would report the following statistics: A) one order by the FISC for the production of tangible things, B) one target of said orders, and C) 33 unique identifiers, representing three targeted email addresses plus 30 non-targeted email addresses.

**Figure 16a: Title V “Traditional” Business Records Orders, Targets, and Unique Identifiers Collected**

Business Records “BR” - Section 501(b)(2)(B)	CY2016	CY2017	CY2018
Total number of orders issues pursuant to applications under Section 501(b)(2)(B)	84	77	<b>56</b>
Estimated number of targets of such orders	88	74	<b>60</b>
Estimated number of unique identifiers used to communicate information collected pursuant to such orders	125,354*	87,834	<b>214,860</b>

See 50 U.S.C. §§ 1873(b)(5), 1873(b)(5)(A), and 1873(b)(5)(B).

\*For the CY2016 report, FBI erroneously provided the estimated number of unique identifiers used to communicate information collected pursuant to orders for PR/TT devices instead of the number of the unique identifiers collected pursuant business records orders. As noted above, FBI erroneously provided the estimated number of unique identifiers used to communicate information collected pursuant to orders for business records orders under the statistics for PR/TT devices.

Figure 16b: “Traditional” Business Records Orders and Targets

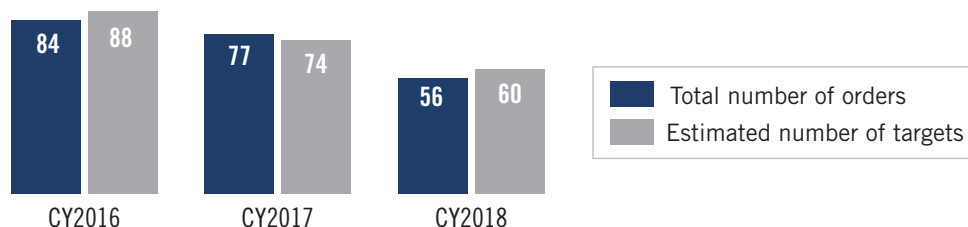
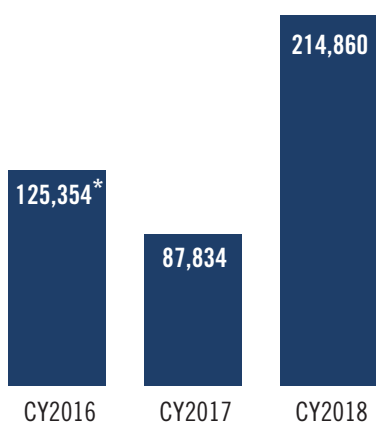


Figure 16c: “Traditional” Business Records Unique Identifiers



See 50 U.S.C. §§ 1873(b)(5), 1873(b)(5)(A), and 1873(b)(5)(B).

\*For the CY2016 report, FBI erroneously provided the estimated number of unique identifiers used to communicate information collected pursuant to orders for PR/TT devices instead of the number of the unique identifiers collected pursuant business records orders. As noted above, FBI erroneously provided the estimated number of unique identifiers used to communicate information collected pursuant to orders for business records orders under the statistics for PR/TT devices.

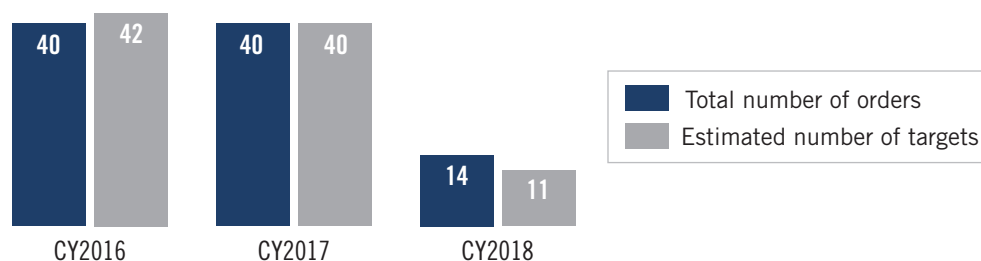
### C. Statistics—Call Detail Record (CDR) Orders, Targets & Identifiers

Call Detail Records (CDRs)—commonly referred to as “call event metadata”—may be obtained from telecommunications providers on an ongoing basis pursuant to 50 U.S.C. § 1861(b)(2)(C). Title V of FISA defines a CDR as session identifying information (such as an originating or terminating telephone number, an International Mobile Subscriber Identity (IMSI) number, or an International Mobile Station Equipment Identity (IMEI)

number), a telephone calling card number, or the time or duration of a call. See 50 U.S.C. § 1861(k)(3)(A). By statute, CDRs provided to the government may *not* include the content of any communication, the name, address, or financial information of a subscriber or customer, or cell site location or global positioning system information. See 50 U.S.C. § 1861(k)(3)(B). CDRs are stored and queried by the service providers. See 50 U.S.C. § 1861(c)(2). After NSA receives the CDRs from the providers pursuant to a FISC order, NSA stores and queries those lawfully obtained CDRs.

**Figures 17a and 17b: CDR Orders and Targets**

Business Records (BRs)—Section 501(b)(2)(B)	CY2016	CY2017	CY2018
Total number of orders issues pursuant to applications under Section 501(b)(2)(C)	40	40	<b>14</b>
Estimated number of targets of such orders	42	40	<b>11</b>



See 50 U.S.C. §§ 1873(b)(6) and 1873(b)(6)(A).

**CHANGES IN TECHNICAL CAPABILITIES TO COUNT UNIQUE IDENTIFIERS.** While the USA FREEDOM Act directs the government to provide a good faith estimate of “the number of unique identifiers used to communicate information collected pursuant to” orders issued in response to CDR applications (see 50 U.S.C. § 1873(b)(5)(B)), in the past, the government did not have the technical ability to isolate the number of unique identifiers within records received from the providers. Since the previous *Annual Statistical Transparency Report*, NSA developed a new technical solution to allow NSA to produce a good faith estimate of the number of unique identifiers. This new technical solution was put into place after the deletion of records in May 2018, so NSA will provide this partial-year count. The deletion of records was publicly discussed in a [June 28, 2018 public notice by NSA](#) and is also discussed below.

In previous years, this report has included an alternate metric that represents the number of records received from the provider(s) and stored in NSA repositories (records that fail at any of a variety of validation steps are not included in this number). CDRs covered by § 501(b)(2)(C) in-

clude call detail records created before, on, or after the date of the application relating to an authorized investigation.

Both metrics are included in this report. NSA counting for CY2018 includes (1) the total number of CDRs received for the year as we have reported in previous years, as illustrated in Figure 19 and (2) the unique identifiers within the CDRs received for the portion of the year NSA was able to count them, as illustrated in Figure 20.

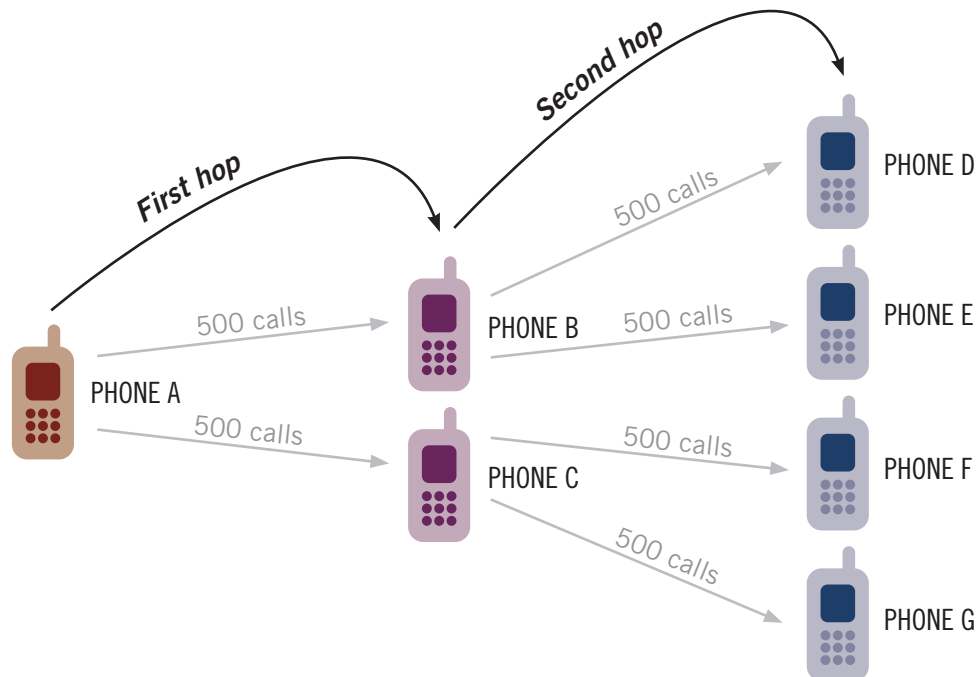
**THE ESTIMATED NUMBER OF CDRS RECEIVED FROM PROVIDERS.** As explained in the [2016 NSA public report on the USA FREEDOM Act](#), the metric provided is over-inclusive because the government counts each record separately *even if the government receives the same record multiple times* (whether from one provider or multiple providers). Additionally, this metric includes duplicates of unique identifiers – i.e., because the government lacked the technical ability to isolate unique identifiers, the statistic counts the number of records even if unique identifiers are repeated. For example, if one unique identifier is associated with multiple calls to a second unique identifier, it will be counted multiple times. Similarly, if two different provid-



ers submit records showing the same two unique identifiers in contact, then those would also be counted separately. This statistic includes records that were received from the providers in CY2018 for all orders active for any portion of the calendar year, which includes orders that the FISC approved in CY2017. Furthermore, while the records are

received from domestic communications service providers, the records received are for domestic and foreign numbers. More information on how NSA implements this authority can be found in the DCLPO report, in particular see [page 5 for a description and illustration of the USA FREEDOM Implementation Architecture.](#)

**Figure 18: Call Event Hop Scenario and Method of Counting**



Target uses **Phone Number A** which is the FISC-approved selector in the FISC order. This would be counted as **1 order, 1 target, 7 unique identifiers (phone numbers A, B, C, D, E, F, G)** and, assuming 500 calls between each party (1,000 records), **6000 CDRs**. CDRs may include records for both sides of a call (for example, one call from **Phone Number A** to **Phone Number B** could result in 2 records).

Assume an NSA intelligence analyst learns that phone number (**Phone Number A**) is being used by a suspected international terrorist (target). **Phone Number A** is the “specific selection term” or “selector” that will be submitted to the FISC (or the Attorney General in an emergency) for approval using the “reasonable articulable suspicion” (RAS) standard. Assume that one provider (provider X) submits a record showing **Phone Number A** called unique

identifier **Phone Number B**—what is referred to as a “call event.” This is the “**first hop**.” In turn, assume that NSA submits the “first-hop” **Phone Number B** to the provider X, and finds that unique identifier was used to call another unique identifier **Phone Number D**. This is the “**second-hop**.” If the unique identifiers call one another multiple times, then multiple CDRs are produced and duplication occurs. Additionally, the government may receive multiple

CDRs for a single call event. NSA may also submit the specific selection **Phone Number A** to another provider (provider Y) who may have CDRs of the same call events.

Not all CDRs provided to the government will be for domestic numbers. The targeted “specific selec-

tion term” could be a foreign number, could have called a foreign number or the “first-hop” number could have called a foreign number; thus, these CDRs statistics contain both domestic and foreign number results. Furthermore, CDRs provided to the government include call events with business entities, such as calls for marketing purposes.

**Figure 19: CDRs Received Arising from Such Targets**

Call Detail Records (CDRs)—Section 501(b)(2)(C)	CY2016	CY2017	CY2018
Estimated number of call detail records arising from such targets that NSA received from providers pursuant to Section 501(b)(2)(C) and stored in its repositories*	151,230,968	534,396,285	<b>434,238,543</b>

\*While the statute directs the government to count the unique identifiers, until May of 2018, the government was not technically able to isolate the number of unique identifiers; thus, the number reported above counts total CDRs received for the year and includes duplicate records. Additionally, the number of records contains both domestic and foreign numbers, including numbers used by business entities for marketing purposes.

**THE ESTIMATED NUMBER OF UNIQUE IDENTIFIERS IN THE CDRS RECEIVED.** On June 28, 2018, NSA issued [a public notice](#) stating that on May 23, 2018, NSA began deleting all CDRs acquired since 2015 under Section 501(b)(2)(C) of FISA. NSA deleted the CDRs because earlier in 2018 NSA analysts noted technical irregularities in some data received from telecommunications service providers. These irregularities also resulted in the production to NSA of some CDRs that NSA was not authorized to receive. Because it was infeasible to identify and isolate properly produced data, NSA concluded that it should not use any of the CDRs. Consequently, NSA, in consultation with the Department of Justice and the ODNI, decided that the appropriate course of action was to delete all CDRs. NSA notified the Congressional oversight committees, the Privacy and Civil Liberties Oversight Board, and the Department of Justice of this decision. The Department of Justice, in turn, notified the Foreign Intelligence Surveillance Court. The root cause of the specific problem that led to the deletion was addressed at that time. Additionally, NSA reviewed and revalidated its intelligence reporting to ensure that the reports were based on properly received CDRs.

During the reporting period, NSA subsequently re-submitted the already FISC-approved selectors to the providers and also submitted new selectors that were approved by the FISC. NSA ingested and stored CDRs produced by the providers in response to these submissions during CY2018. Additionally, during this time, NSA implemented a new technical means of counting the unique identifiers as opposed to counting all records stored in NSA’s repositories. The new counting process was applied as the records were delivered by the providers beginning on May 23, 2018, when the process was initiated.

The new process counts each type of identifier separately, and includes counts for phone numbers, International Mobile Subscriber Identities (IMSI), and International Mobile Equipment Identities (IMEIs). An IMSI is a 15-digit number associated with the SIM card in a mobile phone. An IMEI identifies the specific physical device, much like a serial number. In the CDRs NSA receives under UFA, IMSIs and IMEIs are associated with a phone number, so the phone number count below represents the number of unique phones associated with UFA CDRs.

**Figure 20: Unique Identifiers in the CDRs Received**

Call Detail Records (CDRs)—Section 501(b)(c)(C)	23 May to 31 December 2018
The number of unique identifiers used to communicate information collected pursuant to such orders under Section 501(b)(2)(C)*	19,372,544 Phone Numbers, which are associated with 7,285,362 IMSIs and 5,305,578 IMEIs

\*Identifiers include both domestic and foreign numbers, including numbers used by business entities for marketing purposes.

### *D. Statistics—Call Detail Record Queries*

**THE NUMBER OF SEARCH TERMS ASSOCIATED WITH A U.S. PERSON USED TO QUERY THE CDR DATA.** In 2018, NSA streamlined and upgraded its analytic tools to improve performance and compliance capabilities. This gave NSA analysts an increased ability to group related query terms together and run those query terms against multiple repositories that the analyst is authorized to query. NSA analysts must still comply with all applicable restrictions, controls, and training that apply to each query term and each repository.

Due to the technical parameters of the tool, in order to generate a count of CDR queries, NSA must count all query terms, even if query terms would never return CDR results (e.g. using an email address as a query term will never return a hit from CDR data). Additionally, the parameters of the tool do not allow NSA to distinguish which specific query terms are U.S. persons and which are not when multiple query terms are used. For example, a single query using 20 query terms counts as 20, even if only one of those terms is a U.S. person phone number, and the remaining 19 are either not associated with a U.S. person or are email addresses.

**Figure 21: CDRs—U.S. Person Query Terms**

Call Detail Records (CDRs)—Section 501(b)(2)(C)	CY2016	CY2017	CY2018
Estimated number of search terms that included information concerning a U.S. person that were used to query any database of call detail records obtained through the use of such orders.*	22,360	31,196	<b>164,682</b>

See 50 U.S.C. § 1873(b)(6)(C).

\* Consistent with § 1873(d)(2)(A), this statistic does not include queries that are conducted by the FBI.

# National Security Letters (NSLs)

## A. National Security Letters

In addition to statistics relating to FISA authorities, we are reporting information on the government's use of National Security Letters (NSLs). The FBI is statutorily authorized to issue NSLs for specific records (as specified below) only if the information being sought is relevant to a national security investigation. NSLs may be issued for four commonly used types of records:

- i. telephone subscriber information, toll records, and other electronic communication transactional records, *see* 18 U.S.C. § 2709;
- ii. consumer-identifying information possessed by consumer reporting agencies (names, addresses, places of employment, institutions at which a consumer has maintained an account), *see* 15 U.S.C. § 1681u;
- iii. full credit reports, *see* 15 U.S.C. § 1681v (only for counterterrorism, not for counterintelligence investigations); and
- iv. financial records, *see* 12 U.S.C. § 3414.

## B. Statistics—National Security Letters and Requests for Information

**COUNTING NSLs.** Today we are reporting (1) the total number of NSLs *issued* for all persons, and (2) the total number of requests for information (ROI) contained within those NSLs. When a single NSL contains multiple ROIs, each is considered a “request” and each request must be relevant to the same pending investigation. For example, if the government issued one NSL seeking subscriber information from one provider and that NSL identified three e-mail addresses for the provider to return records, this would count as *one* NSL issued and *three* ROIs.

### National Security Letters

- Not authorized by FISA but by other statutes.
- Bulk collection is prohibited, however, by the USA FREEDOM Act.
- FBI may only use NSLs if the information sought is relevant to international counterterrorism or counterintelligence investigation.

- **THE DEPARTMENT OF JUSTICE'S REPORT ON NSLs.** In April 2019, the Department of Justice released its [\*Annual Foreign Intelligence Surveillance Act Report\*](#) to Congress. That report, which is available online, provides the number of requests made for certain information concerning different U.S. persons pursuant to NSL authorities during calendar year 2018. The Department of Justice's report provides the number of individuals subject to an NSL whereas the ODNI's report provides the number of NSLs issued. Because one person may be subject to more than one NSL in an annual period, the number of NSLs issued and the number of persons subject to an NSL differs.

**WHY WE REPORT THE NUMBER OF NSL REQUESTS INSTEAD OF THE NUMBER OF NSL TARGETS.** We are reporting the annual number of requests for multiple reasons. First, the FBI's systems are configured to comply with Congressional reporting requirements, which do not require the FBI to track the number of individuals or organizations that are the subject of an NSL. Even if the FBI systems were configured differently, it would still be difficult to identify the number of specific individuals or organizations that are the subjects of NSLs. One reason for this

is that the subscriber information returned to the FBI in response to an NSL may identify, for example, one subscriber for three accounts or it may identify different subscribers for each account. In some cases this occurs because the identification information provided by the subscriber to the provider may not be true. For example, a subscriber may use a fictitious name or alias when creating the account. Thus, in many instances, the FBI never identifies the actual subscriber of an account. In other cases, this occurs because individual subscribers may identify themselves differently for each account (e.g., inclusion of middle name, middle initial, etc.) when creating an account.

We also note that the actual number of individuals or organizations that are the subject of an NSL is different than the number of NSL requests. The

FBI often issues NSLs under different legal authorities, e.g., 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709, for the same individual or organization. The FBI may also serve multiple NSLs for an individual for multiple facilities (e.g., multiple e-mail accounts, landline telephone numbers and cellular phone numbers). The number of requests, consequently, is significantly larger than the number of individuals or organizations that are the subjects of the NSLs.

As is the case with other statistics in this report, statistics often fluctuate from year to year for a variety of reasons. The IC is committed to sharing statistical data and engaging the public about how the IC uses its national security authorities and for what purposes.

**Figure 22a: NSLs Issued and Requests for Information**

National Security Letters (NSLs)	CY2013	CY2014	CY2015	CY2016	CY2017	CY2018
Total number NSLs issued	19,212	16,348	12,870	12,150	12,762	<b>10,235</b>
Number of Requests for Information (ROI)	38,832	33,024	48,642	24,801	41,579	<b>38,872</b>

See 50 U.S.C. § 1873(b)(6).

**Figure 22b: Total NSLs Issued and Total ROIs Within Those NSLs**

